Spyware

Michael Glenn
Technology Management
Michael.Glenn@Qwest.com

Qwest
Spirit of Service™

Agenda

- Security Fundamentals
- Current Issues
- Spyware Definitions
- Overlaps of Threats
- Best Practices
- What Service Providers are Doing
- References

Qwest
Spirit of Service™

Security Fundamentals

- Every **security decision = economic decision**
  - Basis of military data classification
  - More security = Less accessibility/usability, higher $$$
- Defense in Depth
  - “Defense-In-Depth strategy integrates People, Operations, and Technology capabilities to establish information assurance (IA) protection across multiple layers and dimensions. Successive layers of defense will cause an adversary who penetrates or breaks down one barrier to promptly encounter another Defense-In-Depth barrier, and then another, until the attack ends.” – NSA web site
- Spheres of Protection
  - Enterprise = Greater restriction of data
  - Service Provider = Less restriction of data

Qwest
Spirit of Service™

Security Fundamentals

- Five Information Assurance Pillars
  - Confidentiality
  - Integrity
  - Availability
  - Authenticity (authentication)
  - Non-repudiation

Current Issues

- Viruses
- Worms
- ‘Bots’ or Zombies
- Key Loggers
- E-mail Spam
- SPIM
- Identity Theft
- Auction Fraud
- Loss of Privacy
- Spyware
- Phishing
- DoS/DDoS
- Cyber Extortion
- Theft of Intellectual Property
- Investment Fraud
- International Money Laundering
- Theft of Services

Traditional crimes are migrating to the Internet

Qwest
Spirit of Service™

Spyware

- What is it?
- Everyone has a different definition
- Lots of legislation trying to fix the problem
  - At least 8 different state bills are pending.
  - Several federal bills are in progress.

Qwest
Spirit of Service™

Spyware Definition - Webopedia

- **(n.)** Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet; however, it should be noted that the majority of shareware and freeware applications do not come with spyware. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers.
  www.pcwebopedia.com/TERM/s/spyware.html

Qwest
Spirit of Service™

Spyware Definition - Microsoft

- Spyware is a general term used for software that performs certain behaviors such as advertising, collecting personal information, or changing the configuration of your computer, generally without appropriately obtaining your consent. http://www.microsoft.com/athome/security/spyware/spywarewhat.mspx

- PUS: Potentially Unwanted Software
  Microsoft Anti-Spyware EULA

Qwest
Spirit of Service™

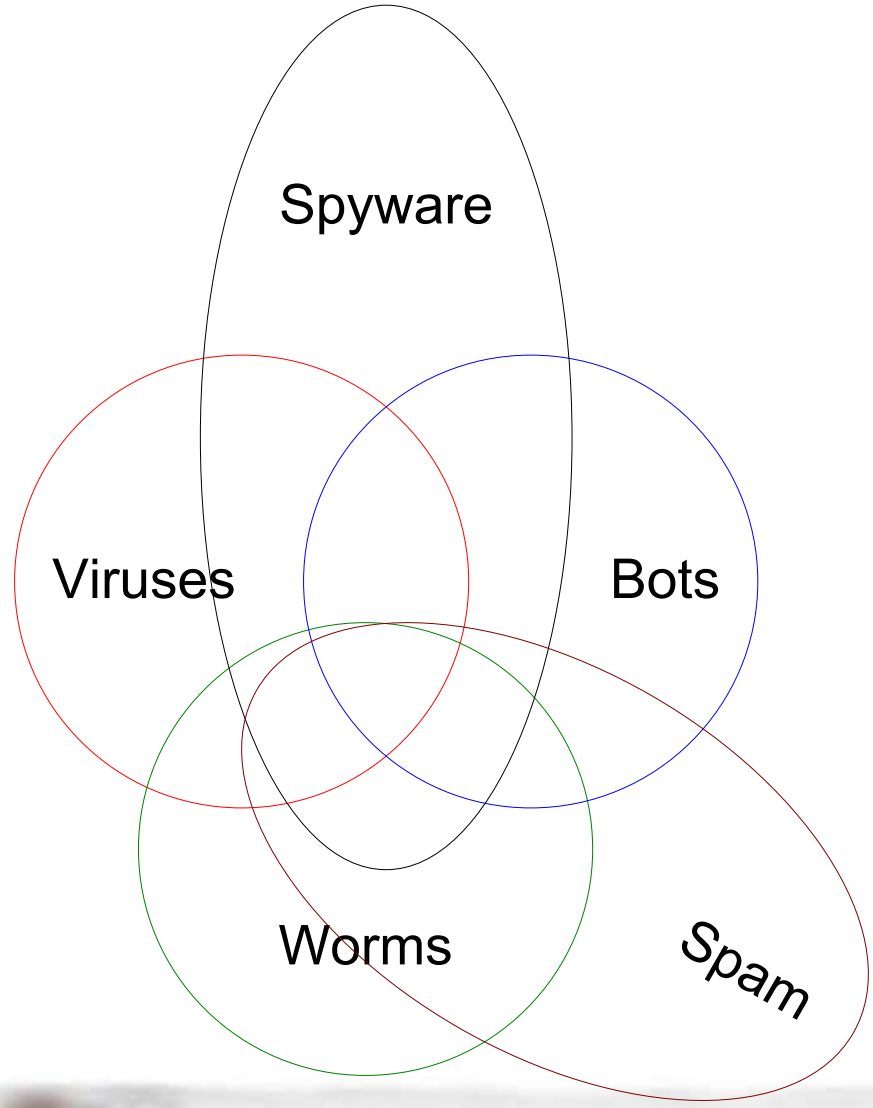
Categories of Spyware

- **Non-malicious** – Generally, programs installed with the user's consent to a EULA or through the setting of cookies in a browser. Usually tracks user preferences and sites visited. It can also present unwanted advertisements to the user or change their computer configuration. Originally developed for targeted advertising.

- **Malicious** – A program that gathers sensitive user information including e-mail addresses, usernames and passwords, SSN, credit card information, and other financial information. Programs gather information through keystroke logging, data file searches, and e-mail monitoring. Many times the software is a blended threat including virus, worm, bot, trojan horse, spam, and other attack vectors.

Spyware is financially driven

Blended Threat



Qwest
Spirit of Service™

Infection Methods

- Web Sites
  - Exploits in IE, Outlook, Mozilla (including Firefox)
- Combination of non-critical exploits
- P2P Sharing Software
- Virus/Worm/Bot infections
- Windows Media Files

Qwest
Spirit of Service™

Phatbot – Bot Swiss Army Knife

- Feature List
  - Ability to polymorph on install
  - Kills up to 600 different programs including anti-virus software and other infections
  - Scans IRC, FTP, HTTP traffic for user logins, passwords and cookies
  - Can steal product codes for Windows and games
  - Harvests e-mail addresses from local system and web
  - Has many different techniques to distribute SPAM
  - Is able to spread using 12-15 different security holes
  - Can be commanded to launch several different types of DoS attacks
  - Can open, delete, upload, download and execute files on the local system
  - Can update itself through plugins or code downloads
  - Uses P2P for control channel
- http://www.lurhq.com/phatbot.html

Best Practices - Enterprise

- Keep your systems patched
- Practice defense in depth
  - Perimeter firewalls: limit inbound and outbound traffic
  - Perimeter IDS/IPS: check both inbound and outbound traffic
  - Host based firewalls
  - Host anti-virus software (on all Windows and Macs)
  - E-mail anti-virus software
  - Regularly run anti-spyware checkups
  - Block unrequested pop-up ads
- Have method to quickly quarantine infected users
- Restrict where users can go on the web
- Published abuse address: abuse@mydomain.gov
  - RFC 2142: Mailbox names for common services, roles and functions

Qwest
Spirit of Service™

What Service Providers Are Doing

- Working cooperatively
  - Monitoring questionable sites
  - Immediately shutting down illegal/AUP violation sites
  - Analyzing malware to understand behavior
- Turning off customers who violate the SP's AUP
- Notifying customers of malware infections
- Quarantining infected residential and small business customers
- Educating users about spyware, identity theft, and good computer security practices.

Qwest
Spirit of Service™

References

- http://spywarewarrior.com
  - Lots of information on spyware
  - http://spywarewarrior.com/asw-features.htm
    - Specific test results on anti-spyware software and recommendations on how to clean and protect your computer.
- http://www.microsoft.com/athome/security/spyware/software/default.mspx
  - Microsoft's new anti-spyware program by Giant. Excellent program but only works for Windows 2000, 2003 and XP.
- http://www.lavasoft.de/
  - Ad-aware anti-spyware software. Free for personal use.
- http://spybot.safer-networking.de/en/index.html
  - Spybot Seach and Destroy. Freeware. Including good spyware blocking tools. Be careful of Spyware Doctor advertising as Spybot S&D.
- http://www.virustotal.com
  - Free service to check suspicious files using multiple virus vendors software.
- http://isc.sans.org/contact.php
  - SANS Internet Storm Center reporting site. If you are seeing suspicious activity, there is a team of technical volunteers who can help you with the issue.
- http://www.qwest.com/about/protection/index.html
  - Good reference on identity theft issues and how to protect yourself.

Qwest Spirit of Service™

Backup Slides

Qwest
Spirit of Service™

Viruses & Worms

Virus: A self-replicating, malicious code that usually requires end user action (click on the attachment) attaches itself to an executable system component and may leave no obvious signs of its presence.

Worm: An independent program that replicates from machine to machine across network connections often clogging networks and information systems as it spreads.

What is the difference?

Viruses usually require you to run them. Worms spread without end user interaction.

Qwest Spirit of Service™

BOTS

Bot = Robot,

- Single instance of a remote controlled application
- The largest botnet found to date was 140,000 computers

There are primarily 3 methods of bot installation:

1) Scan and exploit
2) Come and get it
3) Virus

BotNets can be used for:

Distributed Scanning
Launch Coordinated Attacks
Vulnerability Exploitation
Accessing the Computer

Exchange of Copyrighted Data
Denial of Service (DoS)
Sending Spam
Breaking Codes by Brute Force

Spam and Phishing

- Spam: E-mail, SPIM
  - Accounts for roughly 65% of e-mail
  - 1 billion IM spam (SPIM) messages delivered in 2004
  - Very low take rates still make spam profitable
  - FBI has started aggressive enforcement of CAN-SPAM
- Phishing
  - Never click on a link in an HTML formatted e-mail
  - Practice good risk management when sending e-mails to customers
    - Do not request information directly in the e-mail
    - Do not publish convenient hyperlinks to a web site in the e-mail
  - Report phishing activity to www.antiphishing.org

Qwest
Spirit of Service™